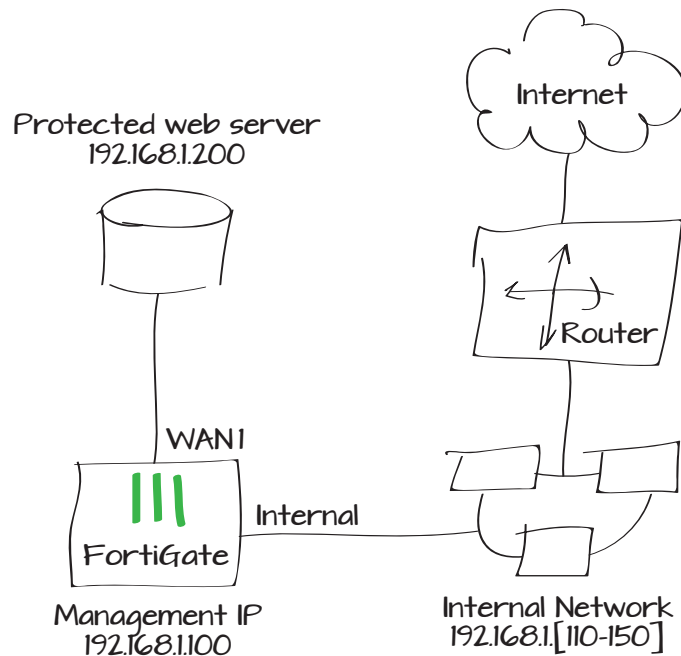


# Using port pairing to simplify transparent mode

When you create a port pair, all traffic accepted by one of the paired ports can only exit out the other port. Restricting traffic in this way simplifies your FortiGate configuration because security policies between these interfaces are pre-configured.

1. Switching the FortiGate unit to transparent mode and adding a static route
2. Creating an internal and wan1 port pair
3. Creating firewall addresses
4. Creating security policies
5. Results



## Switching the FortiGate unit to transparent mode and adding a static route

Go to **System > Dashboard > Status**.

In the **System Information** widget, select **Change**. Set **Operation mode** to **Transparent**.

Log into the FortiGate unit using the management IP (in the example, 192.168.1.100).

Go to **System > Network > Routing Table** and set a static route.

Operation Mode	Transparent ▾
Management IP/Netmask	192.168.1.100/255.255.255.0

Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	192.168.1.99
Comments	Write a comment... 0/255
Priority	0 (0-4294967295)

## Creating an internal and wan1 port pair

Go to **System > Network > Interfaces**.

Create an internal/wan1 pair so that all traffic accepted by the internal interface can only exit out of the wan1 interface.

Name: internal-wan1-port-pair	
Available Members:	Selected Members(must be 2):
<div>dmz</div> <div>ha1</div> <div>ha2</div> <div>mesh.root (SSID: fortinet.mesh.root)</div> <div>mgmt</div> <div>wan2</div>	<div>internal</div> <div>wan1</div>

# Creating firewall addresses

Go to **Firewall Objects > Address > Addresses**.

Create an address for the web server using the web server’s Subnet IP.

Create a second address, with an IP range for internal users.

# Creating security policies

Go to **Policy > Policy > Policy**.

Create a security policy that allows internal users to access the web server using HTTP and HTTPS.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Web\_Server

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.200

Interface

Any

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Internal\_Users

Color

[Change]

Type

IP Range

Subnet / IP Range

192.168.1.110-192.168.1.150

Interface

Any

Show in Address List

☒

Comments

Write a comment... 0/255

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

internal

Source Address

Internal\_Users

Outgoing Interface

wan1

Destination Address

Web\_Server

Schedule

always

Service

HTTP HTTPS

Action

ACCEPT

Create a second security policy that allows connections from the web server to the internal users' network and to the Internet using any service.

## Results

Connect to the web server from the internal network and surf the Internet from the server itself.

Go to **Log & Report > Traffic Log > Forward Traffic** to verify that there is traffic from the internal to wan1 interface.

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

wan1

Source Address

Web\_Server

Outgoing Interface

internal

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Src Interface	Dst Interface	Src	Dst	Sent / Received	Policy I
wan1	internal	192.168.1.200	8.8.8.8	75 B / 286 B	2
wan1	internal	192.168.1.200	8.8.8.8	77 B / 277 B	2
wan1	internal	192.168.1.200	74.125.225.223	1.04 KB / 9.08 KB	2
wan1	internal	192.168.1.200	74.125.226.79	728 B / 2.62 KB	2
wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2
internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1
internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1
internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1
wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2
internal	wan1	192.168.1.111	192.168.1.200	1.46 KB / 2.92 KB	1
internal	wan1	192.168.1.111	192.168.1.200	1.33 KB / 2.70 KB	1
internal	wan1	192.168.1.111	192.168.1.200	1.33 KB / 2.75 KB	1
wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2
wan1	internal	192.168.1.200	74.125.226.67	58.06 KB / 2.06 MB	2

Select an entry for details.

Dst	 74.125.225.223	Virtual Domain	root
Received	9296	Source Country	Reserved
Application Name	 SSL	Sent / Received	1.04 KB / 9.08 KB
Duration	17	Sent	1067
Application Details		Service	HTTPS
Protocol	6	Destination Country	United States
Application Control List	default	Dst Port	443
roll	65531	Status	close
Timestamp	Wed Mar 13 11:05:11 2013	Tran Display	noop
Sequence Number	700150	Policy ID	2
Src Interface	wan1	Src	192.168.1.200
Sent Packets	15	Level	notice 
Application Category	Web.Surfing	Application ID	15895
Src Port	51218	Application Control Action	detected
Log ID	13	Sub Type	forward

Go to **Policy > Monitor > Policy Monitor** to view the active sessions.

